



DOUBLE LAYER CRYPTOGRAPHY USING MULTIPLICATIVE CIPHER AND CHEMICAL PERIODIC TABLE

*Anurag Sinha¹ | Amrit Kumar Bhadani¹

¹Research Scholar, Department of Computer Science, Amity University Jharkhand, Ranchi, Jharkhand (India), 834001

ABSTRACT

According to the present communication system one of the main concerns is secured transformation of data. In this paper we be inclined to propose a two-level encryption in this paper in the first level encryption we use the multiplicative ciphers and Cesar cipher in this level the plain text letters, we shall multiply the key numbers in this level and the second layer encryption we use periodic table exploitation the properties if the quality table, and thus use it for encrypting and decrypting in the same manners. For the information of network security in the second level encryption we will differently types of periodic table properties like atomic no, mass no, IUPAC name, chemical formula, and their properties.

KEYWORDS: Periodic table, Multiplicative cipher, Double Layer cryptography, Random Cipher.

INTRODUCTION:

Cryptography is the examination of cryptosystems [Goldrich, 2000; Katz and Lindell, 2014]. This is the science for information security that transforms into customary plain content. Human unreadable code for instance text and alternate ways around. Are cryptographic money Two subfields, that is, cryptography and cryptanalysis.

A technique made by applying science and rationale to store cryptography Send the data in coded and ensure the schematic isolation about the construction with the objective the recipient can pause and quantify it. Innovation to guarantee data about Making shape text from plain substance is generally called encryption. Cryptography shield for instance data from outcasts is utilized for the adversary and additionally this client Check. Cryptanalysis or unscrambling is to hate science or technique figure Text. The fundamental model of the cryptosystem is spoken in Fig. 1.

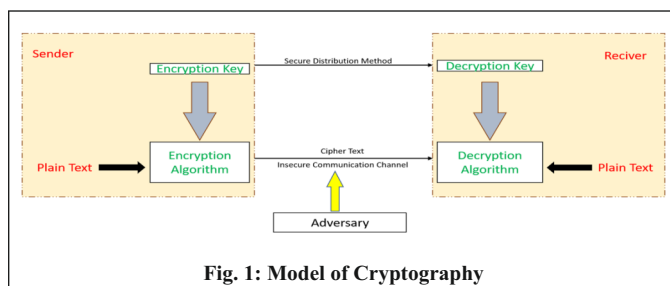


Fig. 1: Model of Cryptography

Normally utilized terms in Cryptography

- **Plaintext:** The first and legitimate substance. As an event, 'Y' necessities to impart a "PC" message to 'Z'. Here, "PC" is the plaintext or the main message.
- **Cipher text:** The substance that cannot be seen by technique for anybody or a foolishness text, model "A@&J9."
- **Encryption:** A pattern of changing clear substance into unclear substance. The method of decipherment needs a decipherment computation and a key. Decipherment occurs on the sender side.
- **Decryption:** A contrary procedure for encode. It is a method of changing over code text into plaintext.
- **Key:** A key is character, number, or an unprecedented character. It is used at the hour of decipherment on the main substance and at the hour of interpret on the code text.

Preliminary:

Validation: The ability of a system to test the personality of the sender.

Privacy: Information conveyed ought to be gotten too handiest by using legitimate social events and not through some other person.

Trustworthiness: Only the endorsed social affairs are permitted to change on sent information.

Non-denial: Is the confirmation that someone cannot keep the authenticity from getting something.

Access Control: Just the endorsed individuals are talented to get right of segment to the given information.

Procedures of Cryptography:

The two key methodologies for encoding data are "symmetric cryptography," which includes the utilization of a comparative key to scramble/interpret information; and "upside down cryptography," which uses public and private keys to encode/unravel information. Examples of symmetric counts are Data Encryption Standard (DES), Triple-DES (3DES), Blowfish, and Progressed Encryption Standard (AES) [20]. The most outstanding strayed counts are RSA furthermore, ELGAMAL Schema.

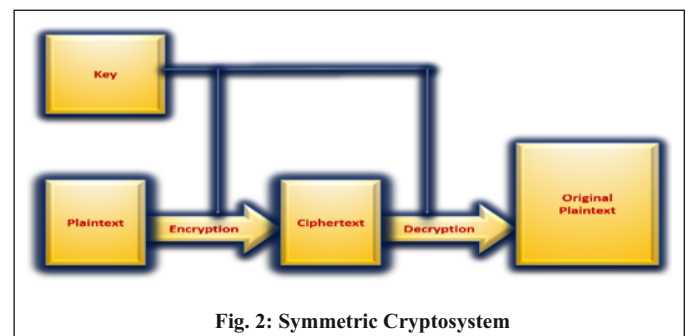


Fig. 2: Symmetric Cryptosystem

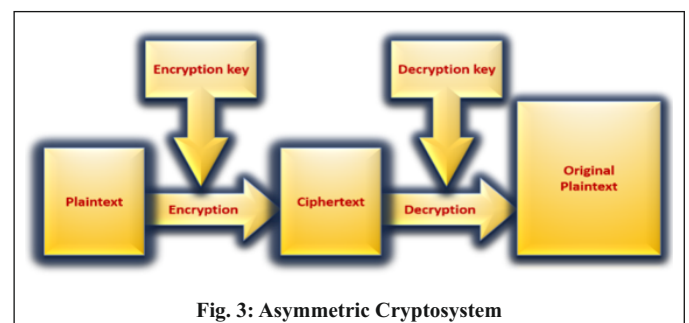
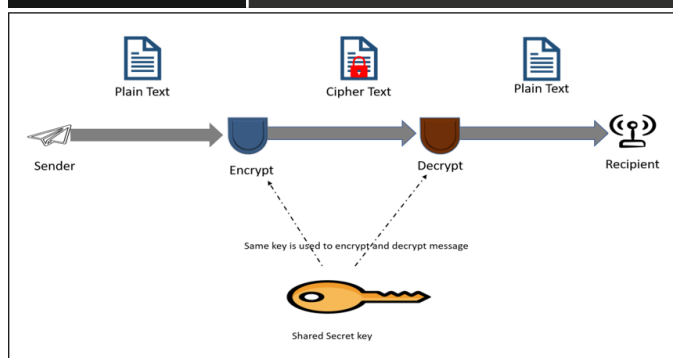


Fig. 3: Asymmetric Cryptosystem

Types of Cryptography:

Secret Key Cryptography: Exactly when a comparative key is used for both encryptions also, unscrambling, DES, Triple DES, AES, RC5, etc., may be the occasions of such encryption, by then that segment is known as secret key cryptography.



Secret Key Cryptography:

Public Key Cryptography: The moment that two keys are used, that is one key for encryption and another key for unravelling, RSA Elliptic curve, etc., may be the occurrences of such encryption, by then that instrument is known as open key cryptography.

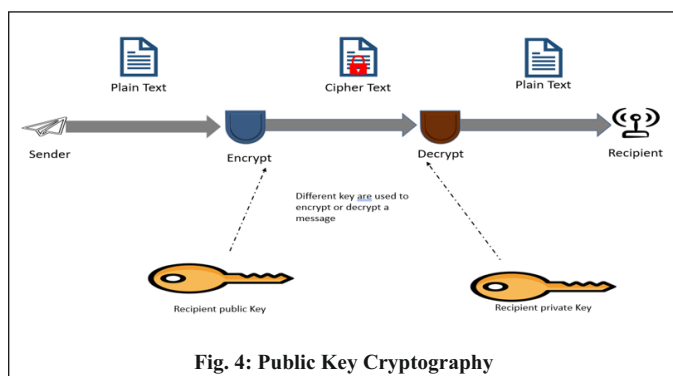


Fig. 4: Public Key Cryptography

LITERATURE SURVEY:

Professor Mukund R. Joshi Renuka Avinash Karkade Planned the paper on the network Security with Cryptography [1].

In this paper some principles of cryptography are mentioned. The redundancy and freshness area unit 2 principles used in cryptography. The message ought to be encrypted at the sender facet however all the encrypted at the sender facet however all the encrypted messages contain some redundancy. The newness use timestamp to get the message. The time is ready for every message the received message is inside the point in time the message is accepted. The message exceeds the point in time before receiving to receiver, those messages area unit discarded. Two categories area unit utilized in cryptography, bilateral and uneven scientific discipline formula totally different key's utilized in sender and receiver facet. In encoding the plain text is regenerate into cipher text. The decipherment is reverse method of encoding, covert cipher text into plain text. Cryptography systems offer privacy and authentication in communication system. Uneven cryptosystems use two sorts of keys one is public key and another one is non-public key. The key distribution is usually recommended by Diffie and Lillian Hellman. Bilateral cryptosystems use data encryption standard and rotor ciphers.

Shyam Nandan Kumar planned review on network security and cryptography [2].

In this paper the categories of security attacks are discussed. Active attacks do some modification information stream. The types of active attacks are modification of message, denial of service, replay and masquerade. Modification of communication. In traffic analysis attacks the message is scan by third party. Unharshness of message contents attacks the message scan by sender and receiver. Some security services are provided for information transmission, information integrity, Data confidentiality, authenticity, nonrepudiation and access management are several the safety services provided by cryptography. Madhumita Panda projected a paper on security in wireless device network victimization cryptological techniques.

In this paper the cryptography is employed in wireless device Network to produce security to the wireless communication. Some security necessities are utilized in wireless device network like confidentiality, authentication, integrity and availability. Some obstacles of device security are employed among a restricted resource. The terribly restricted resources include restricted memory and storage space, power limitation and transmission range. Unreliable communication is additionally one among the obstacles unreliable transfer, conflicts and latency. Unattended operation is one among the obstacles like exposure to physical attacks, managed remotely and lack of central management point even secret is additionally known as secret key. It uses only 1 key on each sender and receiver side uneven cryptography is named as public key cryptography. It uses

totally different keys on both sender and receiver side.

Khandoker Abdul Rahad and Sayed Mohsin Reza planned a paper on the network security with cryptography and ab implementation of Vigenere-multiplicative Cipher.[4]

In this paper the network security as act as an Art of communication provides two types of action: kind Encryption and Decryption. To get information move we need to encode our information by scrambling our data. In the wake of scrambling the data, it is very difficult to comprehend by an outsider.

Robbi Rahim and Ali Ikhwan prepare a project on cryptography technique with Modular Multiplication Block Cipher and Playfair Cipher.[5]

In this paper we tend to prepare associate formula with the combines of Playfair cipher as key substitution and message in plaintext to be encrypted with algorithms MMB, this mix is predicted to extend the protection level of message.

Venkata Krishna Pavan Kalahandi and Yamuna planned a paper on the chemical formula encryption using 7-bit periodic table.[6]

In this paper they planned a brand-new table victimization the properties of the quality table, and therefore use it for encrypting details concerning any drug victimization the drug name, or its formula.

Sriramulu Ajay Babu prepare a paper on the Modification Affine ciphers Algorithms for Cryptography password.[7]

In this paper they build a model of information security for passwords employing a changed technique of affine ciphers. Model analysis of scientific discipline wants this countersign exploitation state transmission diagram.

RELATED WORK:

Multiplicative Ciphers:

It is apparent from the relative straight forwardness with which the Caesar cipher or its speculation to a discretionary number of places of move has been tackled, that such a framework offers next to no security. Allow us to brainstorm an alternate technique for enciphering a message. Rather than adding a vital number to the counterparts of the plain content letters, we will increase by the key number.

Cryptography of Multiplicative Ciphers:

Caesar ciphers are encoded by adding modulo 26 ($C = p + \text{key} \bmod 26$, where C is ciphertext and p is a plain text) and are decoded by adding the converse of the key. It appears to be sensible to consider what might occur if we scrambled by duplicating modulo 26. $C = MP \bmod 26$ where m is known as the multiplicative key. Let us example of 2 as multiplicative key then not of the alphabet appear in the cipher text. The only letter comes in the cipher text are "BDFHJLNPRTVXZ" this seen that we have two copies of all alphabet there has no inverse process in this process. We need a unique key for every alphabet. There have many similar keys they do not have the unique key for every alphabet like as 4,6,8,10, etc.

Let us one more example of 3 as multiplicative key and this time all the letter of the alphabet as exactly one to one mapping. There was also inverse process in this mapping. The ciphertext words are comes from unique plaintext letter.

The reason is few multipliers give a coordinated planning because the answer is that 2 and 26 have a typical divisor of 2, and 4 and 26 have a regular divisor of 2, yet 3 and 26 have no normal divisor.

The lone multipliers that are conceivable are those that bring about balanced mapping. By attempting each of the 26 potential multipliers modulo 26, we would find that solitary 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have inverses. These are the 12 positive whole numbers that are under 26 and moderately prime to 26. In this way, these are just 12 potential multiplicative keys, and one of them is which would make the ciphertext letter set equivalent to the plaintext letter set.

How about we look even more cautiously at augmentation modulo 26. Here is the augmentation table:

Multiplication Modula 26

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	2	4	6	8	10	12	14	16	18	20	22	24	26	2	4	6	8	10	12	14	16	18	20	22	24	26
3	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	26
4	4	8	12	16	20	24	2	6	10	14	18	22	26	4	8	12	16	20	24	2	6	10	14	18	22	26
5	5	10	15	20	25	4	9	14	19	24	3	8	13	14	23	2	7	12	17	22	1	6	11	16	21	26
6	6	12	18	24	4	10	16	22	2	8	14	20	26	6	12	18	24	4	10	16	22	2	8	14	20	26
7	7	14	21	2	9	16	23	4	11	18	25	6	13	18	1	8	15	22	3	10	17	24	5	12	19	26
8	8	16	24	6	14	22	4	12	20	2	10	18	26	8	16	24	6	14	22	4	12	20	2	10	18	26
9	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17	26
10	10	20	4	14	24	8	18	2	12	22	6	16	26	10	20	4	14	24	8	18	2	12	22	6	16	26
11	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15	26
12	12	24	10	22	8	20	6	18	4	16	2	14	26	12	23	10	22	8	20	6	18	4	16	2	14	26
13	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26
14	14	2	16	4	18	6	20	8	22	10	24	12	26	14	2	16	4	18	6	20	8	22	10	24	12	26
15	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11	26
16	16	6	22	12	2	18	8	24	14	4	20	10	26	16	6	22	12	2	18	8	24	14	4	20	10	26
17	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9	26
18	18	10	2	20	12	4	22	14	6	24	16	8	26	14	10	2	20	12	4	22	14	6	24	16	8	26
19	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7	26
20	20	14	8	2	22	16	10	4	24	18	12	6	26	18	14	8	2	22	16	10	4	24	18	12	6	26
21	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5	26
22	22	18	14	10	6	2	24	20	16	12	8	4	26	22	18	14	10	6	2	24	20	16	12	8	4	26
23	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3	26
24	24	22	20	18	16	14	12	10	8	6	4	2	26	24	22	20	18	16	14	12	10	8	6	4	2	26
25	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	26
26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26

Notice that solitary 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have multiplicative inverses modulo 26. Here are the potential multipliers and their inverses.

Numbers	1	3	5	7	9	11	15	17	19	21	23	25
Multiplicative inverse	1	9	21	15	3	19	7	23	11	5	17	25

$1 \times 1 = 1 \pmod{26}$, $3 \times 9 = 27 = 1 \pmod{26}$, $5 \times 21 = 105 = 1 \pmod{26}$, $7 \times 15 = 105 = 1 \pmod{26}$, $11 \times 19 = 209 = 1 \pmod{26}$, $17 \times 23 = 391 = 1 \pmod{26}$, and $25 \times 25 = 625 = 1 \pmod{26}$ what is more, in any case, 2, for instance, does not have a reverse; there could be no number mod 26 that 2 can be duplicated by that will bring about 1.

Periodic Table:

The periodic table is an even plan of the compound components, coordinated

based on their nuclear numbers, electron setups (electron shell model), and repeating chemical properties. Components are introduced arranged by expanding nuclear number (the quantity of protons in the core). The standard type of the table comprises of a lattice of components spread out in 18 sections and 7 lines, with a twofold column of components beneath that.

Today, the intermittent table coordinates 118 named components and recognizes a few more anonymous ones. It has gotten perhaps the most valuable instruments in science, for understudies, however for working physicists as well. It orders the components as indicated by their nuclear number (more on that soon), enlightens us regarding the atomic piece of some random component, depicts how electrons are orchestrated around a given component and permits us to anticipate how one component will respond with another.

For elements with no stable isotopes, the mass number of the isotope with the longest half-life is in parentheses.

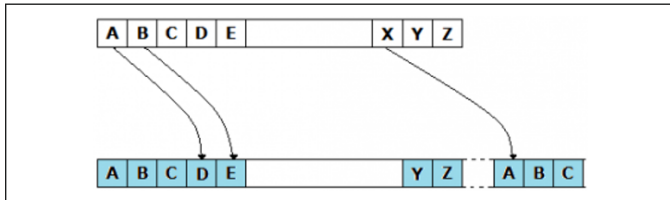
Fig. 5: Periodic Table

(Source: <https://ptable.com/print/periodic-table.pdf>)

History:

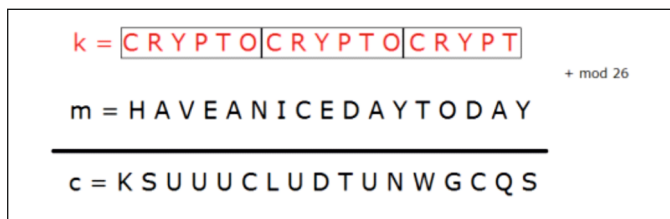
Cryptography is a youthful science. Even though it has been utilized for millennia to shroud mystery message, methodical investigation of cryptography as a science just began around 100 years prior.

Fast forwarding to around 100 BC, Julius Caesar was known to utilize a type of encryption to pass on mystery messages to his military officers posted in the war front. This replacement figure, known as Caesar figure, is maybe the most referenced memorable code in scholarly writing. In replacement figure, each character of the plain content is subbed by another character to shape the code text. The variation utilized by Caesar was a move by 3 code. Each character was moved by 3 spots, so the character 'A' was supplanted by 'D', 'B' was supplanted by 'E', etc. the character would fold over toward the end, so 'X' would be supplanted by 'A'.



It is not difficult to see that such codes rely upon the mystery of the framework and not on the encryption key. When the framework is known, these encoded messages can undoubtedly be unscrambled. Indeed, replacement codes can be broken by utilizing the recurrence of letter in the language.

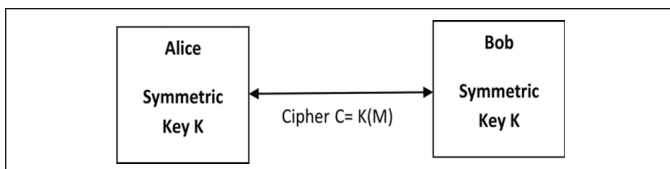
During the 16th century, Vigenere planned a code that was as far as anyone knows the principal figure which utilized as encryption key. On one of his codes, the encryption key was rehased on various occasion traversing the whole message, and afterward the code text was created by adding the message character with the key character modulo 26. As with the Caesar figure, Vigenere code can likewise effectively be broken notwithstanding, vigenere code bought the general concept of bringing encryption key into the image, however it was wretched contrasting this with Caesar figure, the mystery of the message relies upon the mystery of encryption key, as opposed to the mystery of the framework.



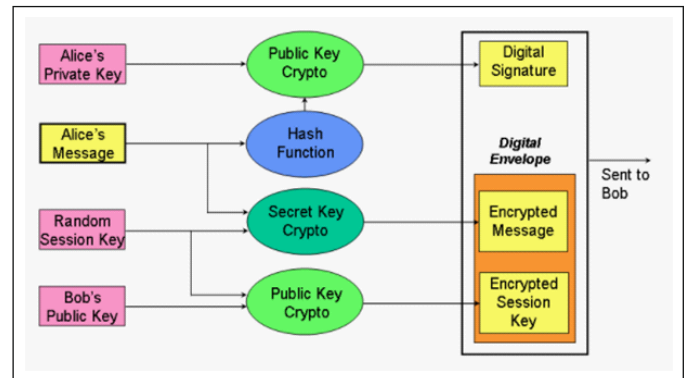
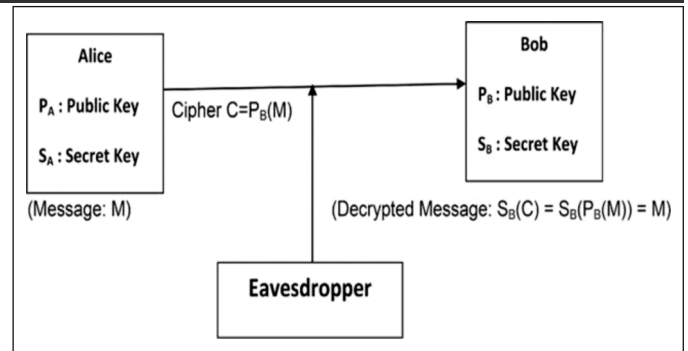
Toward the beginning of the nineteenth century when everything got electric, Hebern planned an electro-mechanical contraption which was known as the Hebern rotor machine. It utilizes a solitary rotor, where the mystery key is installed in a turning circle. The key encoded a replacement table and each critical press from the console brought about the yield of code text. This additionally turned the plate by one score and an alternate table would then be utilized for the following plain content character. This was again broken by utilizing letter frequencies.

Current:

Over the most recent couple of many years, we noticed a huge improvement in the documented of cryptography and organization security. The security and protection the security and security of the enormous measure of imparted data through either wired or remote transmission media. We noticed a critical improvement nearby cryptography and organization security. The region of cryptography concerns secure correspondence among sender and recipient that ought to forestall the snoop to alter or catch private information. Distinctive encryption and decoding methods advanced for this reason. They are comprehensively characterized into two sorts: (a) symmetric-key and (b) public-key cryptosystems. In symmetric-key cryptography, a similar key is divided among the sender and the collector. However, out in the open key cryptography, the sender sends the scrambled information to the recipient utilizing collector's public key. The collector unscrambles the information utilizing his/her own mysterious key. There are a few cryptographic calculations for both symmetric-and public-key cryptosystems. Figure 1 portrays symmetric-key cryptosystem. Figure 2 portrays public-key cryptosystem. In the two figures, the sender is Alice, and the recipient is Bob. The decoded message M is generally known as plain content. The encoded message C is called figure text or in short code.

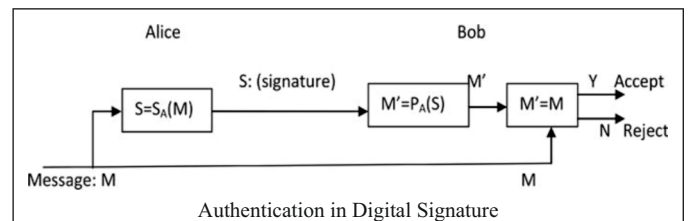


Symmetric key cryptosystem



Public key cryptosystem

Another significant part of secure correspondence is that of nonrepudiation. This is accomplished by methods for advanced mark. In broad daylight key cryptosystem, the sender sends both message and the mark that is the encoded form of the message with the private/secret key of the sender. Figure 3 delineates the advanced mark plot where the computerized signature $S = SA(M)$ is the message scrambled with the mysterious key of Alice. The 2-tuple (S, M) , i.e., the mark alongside the message is sent to Bob. At the less than desirable end, Bob applies the public key of Alice to acquire $M' = PA(S) = PA(SA(M))$ that is assumed be equivalent to M if the mark is legitimate. So, Bob looks at M' and M and acknowledges whether they are equivalent in any case Bob rejects. There are a few varieties of mark plans and many of them utilize cryptographic hash capacities.



The comparable thought of verification is additionally utilized in picture information. A few methods identified with that had advanced as of late in computerized water stamping and steganography. Likewise, there had been a critical improvement in the field of verification utilizing biometric information.

METHODOLOGY:**How Double layer cryptography Work:**

The usage of Double layer encryption procedure is to get the information of the information proprietor by Double layer an encryption in distributed computing. The fundamental procedure is Double Layer Encryption of the archives implies there is two-layer encryption of the information or data. The simple procedure is information proprietor will encode the information multiple times utilizing the produced key what is more, transfer the information to the distributed storage. At the point when the client demands any information from the cloud, the approved client will decode the information multiple times utilizing discharge key and download the information from distributed storage utilizing discharge key. In Double encryption procedure, the RSA calculation is perhaps the best calculation. On this calculation utilize two significant keys that secret key and public key, public key is utilized for scrambling the information as non-clear arrangement and mystery key is utilized for unscrambling the scrambled information. Open key cryptography, RSA calculation is probably the best calculation and is generally used to get information transmission. In RSA, this topsy-turvy key is utilized to lessen this present reality trouble.

The Double Encryption Key Cryptography framework is essentially plan based on key total encryption. Here we are utilizing two keys to encode and decode the information which are secret key and its total key. The information proprietor makes the framework boundary and develops a mysterious key which is public

key. Information can be scrambled multiple times by information proprietor, and he may choose ciphertext related with the plaintext records which need to be encoded. The information proprietor has rights to share the mysterious key from which can create a total key which is use for unscrambling of ciphertext. The decode key can be shipped off end client through mail id in secure way. The confirmed client having secret keys can decode the record.

This paper comprises of five stages which are utilized to play out the activities. These calculations usage having following advances are:

Arrangement: Data Owner makes a record on the worker for sharing of information.

Keygen: This stage is utilized for the age of public key also, secret key. The information proprietor makes a public key to scramble the information over cloud. It additionally makes a mysterious key to decode and download the record.

Encodes and Re-Encrypt: The information proprietor scramble and re-encrypt the information by utilizing the public key. This scrambled information is then

dividing between the cloud.

Concentrate: This stage is utilized to extricate the mysterious keys for decode and download the document from the distributed storage. In any case, other scrambled information stays secure.

Unscramble and Re-Decrypt: The client decodes and re-decode encoded information utilizing the mysterious key.

Disadvantage:

1. Keyword search cause misfortune if data and protection of information is not as much got additionally programmers can undoubtedly assault data.

My proposition improves the security of positioning procedures by giving double layer encryption using multiplicative ciphers and periodic table which beats the security issues of single encryption.

In double layer encryption system we will first use periodic table and then will implement double layer cryptography using multiplicative cipher.

1. Encryption using atomic cipher

PERIODIC TABLE OF THE ELEMENTS

The periodic table displays elements from Hydrogen (1) to Oganesson (118). A callout box for Carbon (C) provides the following information:

- Atomic Number: 6
- Symbol: C
- Name: Carbon
- Electron Configuration: 1s² 2s² 2p²
- Group: 14 (IVA)
- Period: 2
- Block: p-block

Two insets are also present:

- Electron Shells:** A diagram showing the number of electron shells for elements 1 through 18, ranging from 1 to 4 shells.
- Lanthanide and Actinide Series:** Two rows of elements at the bottom of the table, labeled 'Lanthanide' and 'Actinide' respectively.

Encryption comprises in subbing letters (or gathering of letters) addressing a synthetic image by its comparing nuclear number. (Hydrogen H = 1, Helium He = 2, and so forth)

Model: FUSION can be deteriorated in F 9 (Fluor), U 92 (Uranium), Si 14 (Silicium), O 8 (Oxygen), N 7 Nitrogen, so 9,92,14,8,7.

All words can't be crypted as the grouping doesn't contain all letter set letters. To expand the prospects, it is conceivable to utilize the reverse images: 'He = 2' and eH = 2'

decrypt atomic numbers cipher?

Decryption requires to know the periodic table of elements (1 = H, 2 = He, etc.)

Example: 20,37,8,7 for Calcium CA, Rubidium RB, Oxygen O, Nitrogen N gives CARBON

Illustration:

Illustration:
I HATE YOU THATS WHY I DONT WANNA TALK

ENCRYPTED TEXT- 53 1 85 E 39 8 92 90 85 16 74 1 39 53 D8 7 T 74 A7 11 73
L19

DECRYPTION

53185E398929085167413953D87T74A71173L19

I HATE YOU THAT'S WHY I DON'T WANT TO TALK

2. Cryptography using 8-bit periodic table

Table 1: Bitwise allocation of elements

BIT 1	BIT 2,3	BIT 4	BIT 5	BIT 6,7,8
Unique Character for Noble Gas Elements	Group Number	M for Metal	Unique Name of The Group	Mass Number
	Note: For Lanthanides and Actinides Group Number is not fixed.	S for Semi Meta	L -Lanthanide O -Actinide	Note: For Newly Discovered metals, the mass number is yet to be determined. Hence those elements are neglected for further research.
For others, it is 0	Hence default 0 is used	N for Non Metal	A -Alkaline Metal E -Alkaline Earth Metal	
He – H			C -Chalcogen	
Ne – N			P	
Ar – A			Pnicogen	
Kr – K			H -Halogen	
Xe – X			B -Noble Gas	
			θ -No Unique Name	

The typical properties of the substance components are utilized in the development of the 8 – bit occasional table. We utilize the standard occasional table 1 as the base table for the development of this table. The originally chopped is a special character nibbled that has been incorporated distinctly for vowels. It alludes to the principal character of the honorable gas component relegated. Since the gathering number shifts from 1 – 18 the second and third places of the 8 – bit is allocated the gathering number. The mass number of the compound components differs from 1 – 300 and henceforth the last three pieces for the mass number. Spot 4 addresses the metal, nonmetal, semimetal or honorable gas. The fifth piece for the remarkable gathering name. The base for the 8 pieces is given in Table

A	He	0	Hf
E	Ne	1	Hs
I	Ar	2	F
O	Kr	3	Br
U	Xe	4	Ba
B	Li	5	Cs
C	Be	6	Rh
D	Mg	7	Fe
F	Ge	8	Ga
G	O	9	Y
H	P	-	Bh
J	Fr	(Ti
K	W)	Db
L	Os	White	String
M	I	Space	"PA"
N	Rf		
P	Co		
Q	K		
R	Mn		
S	Ag		
T	Mo		
V	Hg		
W	Cr		
X	La		
Y	Pu		
Z	Ir		

Assignment of Characters to Elements

Leave S alone the message to be scrambled. Let S: GOOD BOY

Stage 1 Construct the Periodic table as clarified in area 3. 1.

Stage 2 Construct the Encoding Chart as clarified in area 3.2.

Stage 3 Replace each character in S by its relating substance component from Table - 4 to produce S1.

For the message S, we create

G – Oxygen

O – Krypton

D – Magnesium

B – Lithium

Y – Plutonium

So the S1 is O Kr Ma Li Pu

Leave S alone the message to be scrambled. Let S: GOOD BOY

Stage 4 Replace each character in S1 by its relating 8 – bit code from Table - 3 to produce S2.

The particular 8 bit code can be found for every component from the table 1 . i.e,

Oxygen – 016NC016

Krypton – K18NB084

Magnesium – 002ME024

Lithium – 001MA007

Plutonium – 000MA244

With the goal that S2 is
016NC016K18NB084K18NB084002ME024PA001MA007016NC016000MA
244

Stage 5 Send S2 to the collector.

016NC016K18NB084K18NB084002ME024PA001MA007016NC016000MA
244

s ship off the collector.

Algorithm 2: Decryption Algorithm Decryption is done by reversing the procedure Step 1: Let the key received was

015NP030N18NB020008MT190008MT190K18NB084PA006MT052K18NB
084007MT055008MT190002ME024

Step 2: The code can be split into two parts based on the unique string "PA" which we used for representing the space character i.e., the key has two words.

Word 1: 15NP030N18NB020008MT190008MT190K18NB084

Word 2: 006MT052K18NB084007MT055008MT190002ME024

Step 3: The word can be again split into 8 bit code each bit representing a single unique character

Word 1: 015NP030||N18NB020||008MT190||008MT190||K18NB084

Word 2: 006MT052||K18NB084||007MT055||008MT190||002ME024

Step 4: From the Table – 3 we can identify each 8 bit code representing a unique element. Word 1: HELLO Word 2 : WORLD The string is decrypted as HELLO WORLD.

3. Using random cipher technique:

This code is based off the periodic table of elements. For example, the word 'beer' can be written as:0468

Letters generally come in 2 letter strings, and in this example, the "BE" part is only one digit. You should put a '0' in front of the number '4' (which is Beryllium), or else this can cause confusion. There are very few 3 digit elements, so writing 'beer' as:

004068

would be kind of silly. Instead, for elements 100 - 103, you use the T command (for three). When using commands, there is generally an opening and closing command. In this case, the letter 'T' holds as both the opening and closing. To write "none", you would go:

T102T10

First and Last letter commands

Of course, if we could only limit to the 100 or so abbreviations, it would be impossible to send any message. Instead, you use the A/E and B/E command, where the E serves as the closing mark. The A command takes the first letter of an abbreviation. For example, "A41E08" takes the first letter of element 41 (Nb), which is an N, and connects this to the element 8 (O) to get the word 'no'. The B/E command is almost the same thing, except this takes the last letter of the abbreviation. Do not use this with elements 104+ that have 3 letter abbreviations.

Space

'X' symbolizes space. There are no closing tags for this. The phrase "I at CA" is written as:

53X85X20

I'll also say that punctuation is not changed in this code. Elipses (or "...") are written as:

Missing Letters

Now you probably realize that some of the letters don't appear in any abbreviations at all. The letters are J and Q. There are no closing tags for this. There are two ways to place these in your message if you need to use them:

1) Directly use the letters J and Q. "Jacques" is:
J89Q2B10E16

2) Use the symbols D1 (J) and D2 (Q). "Jacques" is:
D189D292B10E16

Other ways of disguising a message, P.I

The Reverse Function

The reverse function applies for 2 letter abbreviations. You can use it on 1 letter ones to mislead others intercepting messages if you really wanted to. Use the letter 'S' for 'switch' when both opening and closing. For example, the name "Sean"

is:

34S11S

The 'S' reverses the abbreviation of element 11 (Na) to 'an'.

Other ways of disguising a message, P.II

The Column/Row Method

Instead of identifying a square by the number, you can use column/row. There are 18 columns and 7 rows. You are not allowed to use the Lanthanide and Actinide series *** in this method. You use 'CR' for opening and 'YL'. There is no significance in 'YL', except I suppose you can remember it as "You Lost". In the example, the word 'cop' is used:

06CR1602YL15

In the part that states "...CR1602YL...", the 0 before the 2 is optional, as there are only 7 rows, none which require a tens digit. You and your partner may choose what is best for communication.

Note that you can also use RC/LY (which are the reversed commands) for Row-Column. For the previous example, the letter O would be "...RC0216LY..."

The F/F opening and closing statement is fake. Or for you programmers, this is the comment function (or /*...*/). Everything between the two F's are to be ignored! In the example, there is no message at all:

F76193586017852F

Numbers

Method 1:

Use the N/P function to represent numbers. The 'N' stands for number, while the 'P' is just 2 letters after 'N', since the letter in between (O) looks a lot like a number. The number "3141592653" is:

N3141592653P

Method 2:

If you were telling someone your phone number, the above method would make (314)-159-2653 stand out way too much. You can throw in some twists. This part I came up with by looking at squares 104-109 (which are the UN- abbreviations). Note how the last letter in each of these come from some kind of root that coincidentally matches with the unit digit of the square number. So to make number in method 2, you use the U/W tags. The U just means that the idea comes from the UN- series, and the W comes from the "2 after" rule from Method 1. There are two ways to express the numbers between these tags.

1) Use numbers! "3141592653" is:

U3141592653W

This isn't much different from the other case, so take a look at:

2) Use letters! For each digit, you would place a letter that represents that digit. Here is the table:

0 Z Zero
1 M Mono-
2 D/B Di-/Bi-
3 T Tri-
4 Q Quad-
5 P Pent-
6 H Hex-
7 S Sept-
8 O Oct-
9 E En-

For numbers 4 to 9, take a look at the last digit of the abbreviations of elements 104 to 109, respectively. So the number "3141592653" is:

UTMQMPEDHPTW

This is the extent to where I have created this cipher (so far). If anyone has any ideas, feel free to recommend them, and I might add them in.

Why use this?

1) It's made by me. =)

2) There are multiple ways to express each letter.

Good things about this:

1) Good for Periodic Table memorizers

Bad things about this:

1) Recommended to memorize the Periodic Table if you haven't, and quite a bit of commands to remember.

Hope you enjoyed this post! ~ dragon96

practice

Actually, the letter 'V' does appear with element 23, Vanadium.

I really like this cipher. One reason I think it is good is because the same word can be encrypted in multiple ways. Take the word CORN for example. I could encrypt it like this:

2786 (Cobalt + Radon) OR:

060886 (Carbon + Oxygen + Radon) OR:

0608B8607 (Carbon + Oxygen + first letter of Radon + Nitrogen)

SECOND LAYER CRYPTOGRAPHY USING MULTILICATIVE CIPHER

Let us see what goes wrong when we try using 2 as a multiplicative key.

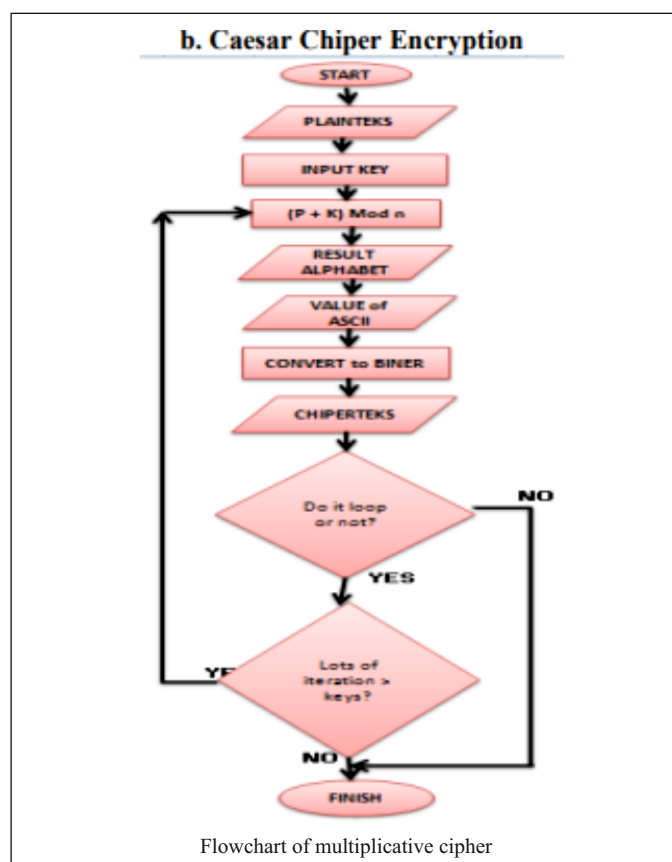














































































































Table 2: Arrangement of multiplicative sequence

a	1	multiplied by 2 modulo 26 is	2	which corresponds to	B
b	2		4		D
c	3		6		F
d	4		8		H
e	5		10		J
f	6		12		L
g	7		14		N
h	8		16		P
i	9		18		R
j	10		20		T
k	11		22		V
l	12		24		X
m	13		26		Z
n	14		2		B
o	15		4		D
p	16		6		F
q	17		8		H
r	18		10		J
s	19		12		L
t	20		14		N
u	21		16		P
v	22		18		R
w	23		20		T
x	24		22		V
y	25		24		X
z	26		26		Z

a	b	c	d	e	f	g	h	i	j	k	l	m	n
													
o	p	q	r	s	t	u	v	w	x	y	z		
													
A	B	C	D	E	F	G	H	I	J	K	L	M	N
													
+	*	+	+	+	+	+	+	+	+	+	+	+	+
O	P	Q	R	S	T	U	V	W	X	Y	Z		
													
.	1	2	3	4	5	6	7	8	9	0	-	=	\
													
~	!	@	#	\$	%	^	&	*	()	_	+	
													
•	✂	✂	✂	✂	✂	✂	✂	✂	✂	✂	✂	✂	•
													
[]	{	}	:	'	:	"	,	.	/	<	>	?
													

Let us now convert the text and no to the following symbols for encryption in view of multiplicative cipher

Notice that not the entirety of the letters of the letters in order show up in the cipher text letters in order; clearly just letters that compare to even numbers can

show up. The cipher text letter set comprises of two duplicates of the letters that compare to the even whole numbers in 1, ... 26; we have two duplicates of the string BDFHJLNPRTVXZ. This plan couldn't be utilized for a code in light of the fact that there is no converse to the cycle; there is no novel approach in reverse from the cipher text to the plaintext. For instance, cipher text N could be either plaintext g or t; it is highly unlikely to tell which is right. Far more detestable, there are 32 potential decoding of BDJLJ. (Would you be able to figure which is known as a polyphonic replacement; more than one plaintext letter may relate to the equivalent cipher ext letter. Albeit in some cases polyphonic replacement is utilized in cryptography, it is by and large just utilized for a couple of letters. Polyphonic replacements don't give remarkable decoding. In the event that the multiplicative key is 2, each cipher text letter compares to two plaintext letters; this is a two-to-one planning. Keep in mind, for a reverse to exist – to have the option to unscramble – we need a coordinated planning.

True to form, all the letters of the letters in order show up in the cipher text letter set. This is a balanced planning. Once more, we might have started with 1 which relates to plaintext an and increased it by 9 modulo 26 which relates to cipher text I. At that point we might have checked 9 additional letters to get the following cipher text letter R, 9 more to get the following cipher text letter A, and so forth. We don't go to a numerous of 26 until we do this interaction multiple times. The way toward encoding by duplicating by 6 modulo 26 doesn't have an converse and would not fill in as a code, yet the way toward scrambling by increasing by 9 modulo 26 has a converse and would fill in as a figure.

Multiplication modulo 26

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26		
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26		
2	2	4	6	8	10	12	14	16	18	20	22	24	26	2	4	6	8	10	12	14	16	18	20	22	24	26		
3	3	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	26	
4	4	4	8	12	16	5	20	24	2	6	10	14	18	22	26	4	8	12	16	20	24	2	6	10	14	18	22	26
5	5	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21	26	
6	6	6	12	18	24	4	10	16	22	2	8	14	20	26	6	12	18	24	4	10	16	22	2	8	14	20	26	
7	7	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	26	
8	8	8	16	24	6	14	22	4	12	20	2	10	18	26	8	16	24	6	14	22	4	12	20	2	10	18	26	
9	9	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17	26	
10	10	10	20	4	14	24	8	18	2	12	22	6	16	26	10	20	4	14	24	8	18	2	12	22	6	16	26	
11	11	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15	26	
12	12	12	24	10	22	8	20	6	18	4	16	2	14	26	12	23	10	22	8	20	6	18	4	16	2	14	26	
13	13	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	
14	14	14	2	16	4	18	6	20	8	22	10	24	12	26	14	2	26	4	18	6	20	8	22	10	24	12	26	
15	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11	26		
16	16	16	6	22	12	2	18	8	24	14	4	20	10	26	16	6	22	12	2	18	8	24	14	4	20	10	26	
17	17	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9	26	
18	18 <td>18</td> <td>10</td> <td>2</td> <td>20</td> <td>12</td> <td>4</td> <td>22</td> <td>14</td> <td>6</td> <td>24</td> <td>16</td> <td>8</td> <td>26</td> <td>18</td> <td>10</td> <td>2</td> <td>20</td> <td>12</td> <td>4</td> <td>22</td> <td>14</td> <td>6</td> <td>24</td> <td>16</td> <td>8</td> <td>26</td>	18	10	2	20	12	4	22	14	6	24	16	8	26	18	10	2	20	12	4	22	14	6	24	16	8	26	
19	19	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7	26	
20	20	20	14	8	2	22	16	10	4	24	18	12	6	26	20	14	8	2	22	16	10	4	24	18	12	6	26	
21	21	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5	26	
22	22	22	18	14	10	6	2	24	20	16	12	8	4	26	22	18	14	10	6	2	24	20	16	12	8	4	26	
23	23	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3	26	
24	24	24	22	20	18	16	14	12	10	8	6	4	2	26	24	22	20	18	16	14	12	10	8	6	4	2	26	
25	25	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	26	
26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	

Notice that only 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have multiplicative inverses modulo 26. Here are the possible multipliers and their inverses: Number 1 3 5 7 9 11 15 17 19 21 23 25 Multiplicative inverse 1 9 21 15 3 7 23 11 5 17 25 11 1 mod $26 \times =$, 3 9 26 1 mod $26 \times =$, 5 21 105 1 mod $26 \times =$, 7 15 105 1 mod $26 \times =$, 11 19 209 1 mod $26 \times =$, 17 23 391 1 mod $26 \times =$, and . But, 2, for example, does not have an inverse; there is no number mod 26 that 2 can be multiplied by that will result in 1.

Here is an example of a multiplicative cipher with multiplicative key 7. Multiplicative cipher Multiplicative key = 7

a	1	7	G
b	2	14	N
c	3	21	U
d	4	2	B
e	5	9	I
f	6	16	P
g	7	23	W
h	8	4	D
i	9	11	K
j	10	18	R
k	11	25	Y
l	12	6	F
m	13	13	M
n	14	20	T
o	15	1	A
p	16	8	H
q	17	15	O
r	18	22	V
s	19	3	C
t	20	10	J
u	21	17	Q
v	22	24	X
w	23	5	E
x	24	12	L
y	25	19	S
z	26	26	Z

The disjoint cycles of the key are (agweikyscuqo)(bntirvxlfpqd)(m)(z).

Here is a frequency chart for a multiplicative cipher with multiplicative key 7.

Frequencies Multiplicative key=7

```

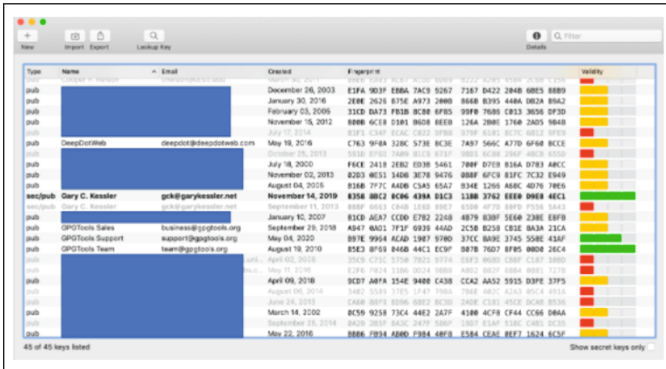
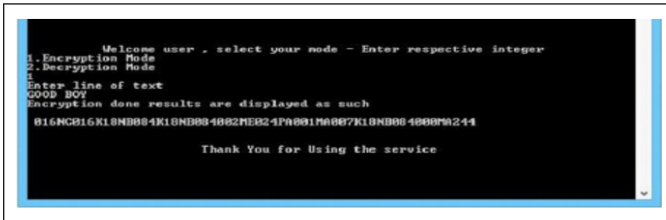
A      11111111
B      11111
C      1111111
D      11111
E      111
F      11111
G      11111111
H      1111
I      1111111111111111
J      11111111111
K      11111111
L
M      111
N      1
O
P      111
Q      111
R
S      11
T      1111111111
U      111
V      1111111111
W      11
X      1
Y
Z

```


RESULTS:

The proposed method is implemented using C++.

Snapshot – 1 provides the encryption for the example GOOD BOY discussed in section C For the received message as discussed in section C 015NP030N18NB020008MT190008MT190K18NB084PA006MT052K18NB084007MT055008MT190002ME024 Snapshot – 2 provides the message decrypted as HELLO WORLD.

**CONCLUSION:**

A parallel string can be of any length and various double strings are accessible out in the open area. So it is hard to track down the distinction between a phony double string and the scrambled one. We have utilized inclusion strategy. So all the preferences of scrambling a message utilizing this strategy applies here too. Additionally since each substance component is changed over into a double string, it is hard for anybody to figure this as a substance recipe since an intermittent table utilizing double string isn't being used.

The intermittent table has 118 components and the characters are arbitrarily appointed in the table. So except if this is known it is hard to decode the message. Likewise every cell of the intermittent table is relegated a 8 – bit code. So except if this is known, unscrambling is absurd. Additionally, occasional table isn't in wide use for encryption, decoding. The proposed technique is additionally easy to use and can be actualized in any programming language. So the proposed strategy is protected for encryption of any instant message

REFERENCES:

- I. Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 36-54). Springer, Berlin, Heidelberg.
- II. Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), 763- 770.
- III. Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. International Journal Of Engineering And Computer Science, 6(4).
- IV. Shipra Jain, Dr.Vishal Bhatnagar. "A novel DNA sequence Dictionary method for securing data in DNA using Spiral Approach and Framework for DNA Cryptography". IEEE International conference on advances in Engineering & Technology Research.,2014.
- V. Disina, Abdulkadir Hassan. "Robust Caesar Cipher against frequency cryptanalysis using bi-directional shifting." Diss. Universiti Tun Hussein Onn Malaysia, 2014.
- VI. Omolara, O. E., A. I. Oludare, and S. E. Abdulahi. "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication." Computer Engineering and Intelligent Systems 5.5 (2014): 34-46.
- VII. Singh, Ajit, Aarti Nandal, and Swati Malik. "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security." International Journal of Advanced Research in Computer Science and Software Engineering 2.12 (2012).
- VIII. Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Caesar and Vigenere cipher." Computational Intelligence and Computing Research (ICICR), 2013 IEEE International Conference on. IEEE, 2013.
- IX. Hadiwibowo. Pengamanan Information and Cryptography - Adding khasanah reading cryptology and information security for the people of Indonesia. Http://hadiwibowo.wordpress.com., December 23, 2006.
- X. Munir, Rinaldi. 2004. Diklat Lecture IF2153 Discrete Mathematics - Fourth Edition. Bandung: Teknik Informatika Study Program, STEI ITB. 2004. Classic Cipher System. http://kur2003.if.itb.ac.id/file/System%20Chiper%20Klasik.doc.

- XI. Krishna moorthy, Dr, and S. Chidam baranathan. "Clever Cardnovel Authentication Protocol (NAUP) in Multi-Computing Internet of Things Environs." (2017).
- XII. Duong, T., & Rizzo, J. (2011, May). Cryptography in the web: The case of cryptographic design flaws in asp. net. In Security and Privacy (SP), 2011 IEEE Symposium on (pp. 481-489). IEEE.
- XIII. Mohamed Saied Emam Mohamed, Albrecht Petzoldt. The shortest Signatures Ever INDOCRYPT2016 2017, LNCS 10095 Springer, pp. 61-77 https://eprint.iacr.org/2016/911.pdf, eprint preprint.
- XIV. Shay Gueron and Nicky Mouha. Simpura v2: A family of efficient permutations using the AES round function, in Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I, 2016, pp. 95:125.
- XV. Albrecht Petzoldt, Alan Szepeieniec, Mohamed Saied Emam Mohamed. A Practical Multivariate Blind Signature Scheme. Financial Cryptography and Data Security 2017, LNCS 10322, Springer, pp. 437-454. http://eprint.iacr.org/2017/131.pdf, eprint preprint.